APPENDIX II

DEFINITIONS

1. For the purpose of this instruction, the following definitions apply:

a. Administrative Vehicle Inspection. A cursory inspection of the contents of a vehicle with full consent of the operator or owner. Administrative inspections are conducted with prior written authorization and direction by the installation or activity commanding officer as to the methods and procedures to be employed.

b. Antiterrorism. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

c. Antiterrorism/Force Protection Plan. Specific measures taken to establish and maintain an antiterrorism/force protection program.

d. Antiterrorism/Force Protection Program. Seeks to reduce the likelihood that Navy-affiliated personnel, their families, facilities, and materiel will be subject to a terrorism attack, and to mitigate the effects of such attacks should they occur.

e. Armed Guard. A person equipped with a firearm and ammunition whose primary function is to protect property and who has qualified with the firearm in an approved weapons qualification course.

f. Auxiliary Security Force (ASF). An armed force composed of local, non-deploying military assets derived from host and tenant commands under the operational control of the host command's security department. The ASF is used to augment the installation's permanent security force during increased threat conditions or when directed by the host command.

g. Critical Communications Facility. A communications facility that is essential to the continuity of operations of the National Command Authority during national emergencies, and other nodal points or elements designated as crucial to mission accomplishment.

h. Commanding Officer. The term "commanding officer" as used throughout this manual includes commanders, directors, officers in charge, etc.

i. Electronic Security Systems. That part of physical security concerned with the safeguarding of personnel and property by use of electronic systems. These systems include,

but are no limited to, intrusion detection systems, automated entry control systems, and video assessment systems.

j. Exception. A written, approved long-term (36 months or longer) or permanent deviation from a specific provision of this instruction. Exceptions require compensatory or equivalent security measures.

k. Facility. A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land.

l. Force Protection. Security programs designed to protect Navy members, civilian employees, family members, facilities, and equipment in all locations and situations, accomplished through the planned and integrated application of combating terrorism, physical security, operations security, personnel protective services, and supported by intelligence, counterintelligence, and other security programs.

m. Incident Response Plan. A set of procedures in place for dealing with the effects of an incident.

n. Installations. Real Department of Defense properties including bases, stations, forts, depots, arsenals, plants (both contractor and government-operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

o. Loss Prevention. Part of an overall command security program dealing with resources, measures and tactics devoted to care and protection of property on an installation. It includes identifying and reporting missing, lost, stolen, or recovered government property, including documents and computer media, and developing trend analyses to plan and implement reactive and proactive loss prevention measures.

p. Navy Activity. Any unit of the Navy shore establishment or operating forces under a commander, commanding officer, or an officer in charge.

q. Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage and theft.

r. Physical Security Inspection. An examination of the physical security and loss prevention programs of an activity to determine compliance with physical security policy. A physical security inspection is normally conducted by a representative of an immediate superior in command. Follow-up action to correct noted deficiencies is required.

s. Physical Security Survey. A specific on-site internal examination/evaluation of physical security and loss prevention programs of an activity to determine the activity's vulnerabilities and compliance with physical security policies. They are used primarily as a management tool by the surveyed command and program manager.

t. Property. All assets including real property; facilities; funds and negotiable instruments; arms, ammunition and explosives; tools and equipment; material and supplies; communications equipment; computer hardware and software; and information in the form of documents and other media; whether the property be categorized as routine or special, unclassified or classified, non-sensitive or sensitive, conventional or nuclear, critical, valuable, or precious.

u. Restricted Area. An area to which entry is subject to special restrictions or control for security reasons, or to safeguard property or material. This does not include those designated areas restricting or prohibiting overflight by aircraft. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation/activity properly posted, and shall employ physical security measures.

v. Security Force. That portion of a security organization at a Navy installation/activity comprised of active duty military, civilian police/guard, or contract guard personnel, tasked to provide physical security and/or law enforcement. The size and composition of the security force will depend on the size of the installation/activity, geographic location, criticality of assets, vulnerability and accessibility, as determined by the installation/activity commanding officer.

w. Survivability. The ability to withstand or repel attack, or other hostile action, to the extent that essential functions can continue or be resumed after onset of hostile action.

x. Systems Security Engineering (SSE). An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. SSE uses mathematical, physical, and related scientific disciplines, and the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of the system to security threats.

y. Threat Assessment Plan. The process used to conduct a threat analysis and to develop a threat assessment.

z. Waiver. A written temporary relief, normally for a period of 1 year, from specific standards imposed by this instruction, pending actions or accomplishment of actions which will result in conformance with the standards. Interim compensatory security measures are required.